**Patent number:** DE10040855 (A1)

**Publication date:** 2002-03-14

**Inventor(s):** JUNG PETER [DE]

**Applicant(s):** INFINEON TECHNOLOGIES AG [DE]

**Classification:**

**- international:** *G06F21/00; H04L29/06;* G06F21/00; H04L29/06; (IPC1-7): G06F12/14; G06F15/173; H04L9/32

**- european:** G06F21/00N5A2B; H04L29/06S8F

**Application number:** DE20001040855 20000821

**Priority number(s):** DE20001040855 20000821

**Also published as:**

DE10040855 (B4)

**Cited documents:**

DE19533209 (A1)

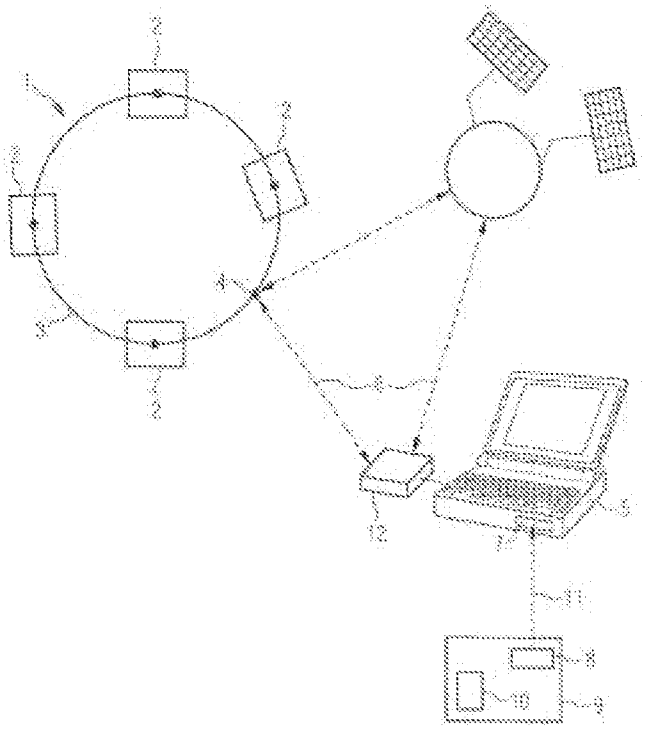
**View INPADOC patent family**

**View list of citing documents**

Report a data error here

Abstract of **DE 10040855 (A1)**

An identification computer (9) with a biometric e.g. fingerprint sensor (10), verifies authenticity of the user and transmits associated password, access data and control command to a user terminal (5) through e.g. a Bluetooth communication interface (7,8). The user terminal establishes connection with the local network (1) using the access data and the password.



PH: DE020188WO MAT

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 40 855 A 1**

(51) Int. Cl.[7]:
**G 06 F 12/14**
G 06 F 15/173
H 04 L 9/32

(21) Aktenzeichen: 100 40 855.9
(22) Anmeldetag: 21. 8. 2000
(43) Offenlegungstag: 14. 3. 2002

(71) Anmelder:
Infineon Technologies AG, 81669 München, DE

(74) Vertreter:
Epping, Hermann & Fischer, 80339 München

(72) Erfinder:
Jung, Peter, 67697 Otterberg, DE

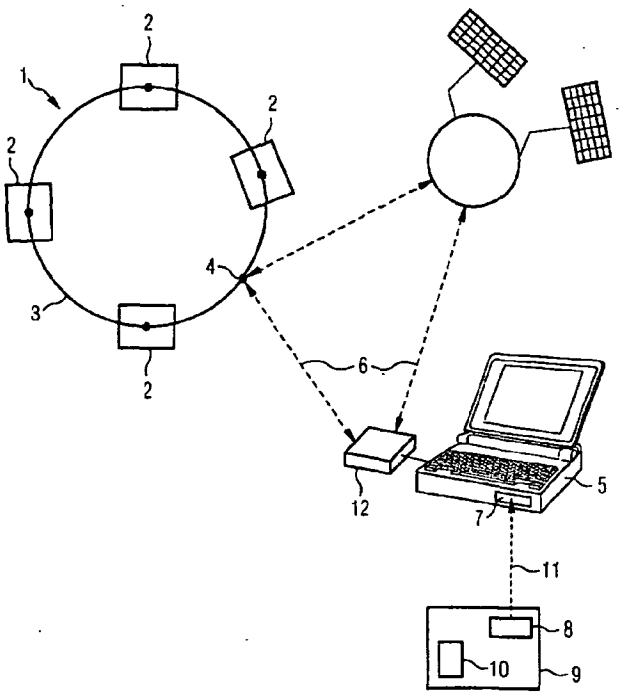
(56) Entgegenhaltungen:
DE 195 33 209 A1

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Netzwerkanordnung

(57) Die Erfindung betrifft eine Netzwerkanordnung mit einem lokalen Computernetzwerk (1), einem Einzelrechner (5) und einem Identifizierungs-Computer (9). Der Einzelrechner (5) weist Mittel (12) zum Aufbau einer Verbindung zu dem lokalen Netzwerk (1) auf. Der Identifizierungs-Computer (9) kann über eine Kommunikationsschnittstelle mit dem Einzelrechner (5) Daten und Steuerbefehle austauschen. In dem Identifizierungs-Computer (9) sind Zugangsdaten für das Computernetzwerk (1) gespeichert und über einen Steuerbefehl von dem Identifizierungs-Computer an den Einzelrechner (5) wird ein automatischer Verbindungsaufbau zu dem Computernetzwerk (1) mit Zugangsdaten und Paßwort von dem Identifizierungs-Computer durchgeführt. In einer Weiterbildung weist der Identifizierungs-Computer einen biometrischen Sensor zur Benutzerauthentisierung auf.




DE 100 40 855 A 1

DE 100 40 855 A 1

Beschreibung

[0001] Die Erfindung betrifft eine Netzwerkanordnung zur Verbindung eines Einzelrechners mit einem lokalen Computernetzwerk.

[0002] In vielen Anwendungsfällen sind Einzelrechner einer Benutzergruppe in einem lokalen Computernetzwerk zusammengeschlossen. Dies ermöglicht die Kommunikation der Rechner untereinander sowie den Zugriff auf gemeinsame Ressourcen wie Datenbestände und Drucker. Trotzdem soll in der Regel die Möglichkeit bestehen, sich von außen in das lokale Netzwerk einzuklinken, um so auch von einem entfernt plazierten-Einzelrechner die Möglichkeit zu haben, auf die Ressourcen des Netzwerkes zuzugreifen. Gerade durch die zunehmende Verbreitung von tragbaren Computern, den sogenannten Notebooks oder Laptops, kann so beispielsweise auf einer Dienstreise fast unter Bürobedingungen gearbeitet werden. Auch die beginnende Einführung von Arbeitszeitmodellen mit teilweiser Heimarbeit erfordert es, von zu Hause aus auf das lokale Computernetzwerk der Firma zugreifen zu können.

[0003] Allerdings muß sichergestellt werden, daß sich nur berechtigte Benutzer in das lokale Computernetzwerk einwählen. Außerdem ist eine Vielzahl von Zugangsdaten notwendig, um auf technischer Ebene die Kommunikation zwischen dem Einzelrechner und dem Computernetzwerk herzustellen. Die sogenannte Fernregistrierung wird bisher von Hand durchgeführt. Dieses Vorgehen ist aber zum einen langwierig und zum anderen fehlerträchtig. Des weiteren ist es anfällig für unautorisierte Verwendung durch Dritte, da oft das Paßwort auf der Festplatte gespeichert oder schriftlich notiert wird. Auch der Einsatz spezieller Software zum Ausprobieren oder Erraten des Paßwortes führt oft zum unberechtigten Zugriff Dritter auf das Computernetzwerk unter Ausnutzung der Möglichkeit der Fernregistrierung.

[0004] Aufgabe der Erfindung ist es daher, eine Netzwerkanordnung vorzuschlagen, bei der die Fernregistrierung vereinfacht und die Sicherheit gegen unautorisierte Verwendung durch Dritte erhöht wird.

[0005] Dieses Ziel wird durch eine Netzwerkanordnung erreicht mit

- einem lokalen Computernetzwerk,
- einem Einzelrechner, der Mittel zum Aufbau einer Verbindung zu dem lokalen Netzwerk aufweist, und
- einem Identifizierungs-Computer, der über eine Kommunikationsschnittstelle mit dem Einzelrechner Daten austauschen kann, wobei in dem Identifizierungs-Computer Zugangsdaten zu dem lokalen Netzwerk gespeichert oder erzeugbar sind und wobei auch durch Übermittlung eines Steuerbefehls von dem Identifizierungs-Computer an den Einzelrechner ein Verbindungsaufbau zwischen dem Einzelrechner und dem Computernetzwerk und eine Registrierung im lokalen Computernetzwerk mit den Zugangsdaten durchgeführt werden.

[0006] Die Zugangsdaten zu dem lokalen Computernetzwerk sind also nicht von Hand einzugeben, sondern sind auf dem Identifizierungs-Computer, der die Form einer Chipkarte haben kann, gespeichert. Fehler bei der Eingabe der Zugangsdaten sind somit ausgeschlossen. Der Aufbau einer Verbindung zwischen dem Einzelrechner und dem Computernetzwerk kann auf Knopfdruck geschehen, da der Einzelrechner durch den Identifizierungs-Computer fernsteuerbar ist, nämlich durch Übermittlung eines Steuerbefehls eine Verbindung herstellt.

[0007] Der Benutzer und Besitzer des Identifizierungs-Computers ist auch nicht darauf angewiesen, immer denselben Einzelrechner zu verwenden. Unter der Voraussetzung, daß die entsprechende Datenfernübertragungssoftware installiert ist und eine Schnittstelle zur Kommunikation mit dem Identifizierungs-Computer besteht, kann die Verbindung von jedem beliebigen Einzelrechner aus aufgebaut werden.

[0008] Zur Erhöhung der Zugangssicherheit ist in einer Weiterbildung der Identifizierungs-Computer um eine Benutzerauthentisierungseinheit erweitert. In einer besonders vorteilhaften Ausgestaltung ist dies ein biometrischer Sensor, vorzugsweise ein Sensor zur Erkennung eines Fingerabdrucks.

[0009] Die Verbindung zwischen dem Identifizierungs-Computer und dem Einzelrechner erfolgt in besonders einfacher Weise durch eine Blue Tooth-Schnittstelle.

[0010] Die Erfindung wird nachfolgend anhand eines Ausführungsbeispieles näher erläutert. Die Figur zeigt schematisch die Elemente der Netzwerkanordnung und die Kommunikationspfade zwischen den Elementen.

[0011] In dem Ausführungsbeispiel gemäß der Figur sind mehrere Computer **2** über eine Datenleitung **3** zu einem lokalen Computernetzwerk **1** zusammengeschlossen. Außerdem ist ein zusätzlicher Knoten **4** vorgesehen, über den sich weitere Computer von außen in das lokale Computernetzwerk **1** einwählen können. Dies ist möglich mit einem Einzelrechner **5**, der Mittel zum Aufbau einer Verbindung **6** zu dem lokalen Computernetzwerk **1** aufweist. Dazu notwendig ist eine Kommunikationsschnittstelle, beispielsweise ein Modem **12**. Die Verbindung kann dabei sowohl über das Festnetz als auch über Mobilfunk erfolgen. Der Einzelrechner weist darüber hinaus eine weitere Kommunikationsschnittstelle **7** auf, über die Daten und Steuerbefehle entgegen genommen werden können. Der Einzelrechner ist so ausgerüstet, daß der Verbindungsaufbau zwischen dem Einzelrechner **5** und dem lokalen Computernetzwerk **1**, also die Verbindung **6**, über einen Steuerbefehl und einer auf dem Einzelrechner **5** installierten Software automatisch hergestellt werden kann. Erfindungsgemäß wird dieser Steuerbefehl von einem Identifizierungs-Computer **9** gesendet. Dazu weist der Identifizierungs-Computer **9** ebenfalls eine Kommunikationsschnittstelle **8** auf, über die er mit der Kommunikationsschnittstelle **7** des Einzelrechners **5** kommunizieren kann. In dem Identifizierungs-Computer **9** sind die Zugangsdaten zu dem Computernetzwerk **1** hinterlegt.

[0012] Zusätzlich ist in dem Identifizierungs-Computer eine Benutzerauthentisierungseinheit **10** vorgesehen, um zu verhindern, daß ein unbefugter Nutzer, der in den Besitz des Identifizierungs-Computers gelangt ist, sich in das lokale Computernetzwerk **1** einwählen kann. Die Benutzerauthentisierungseinheit **10** ist im vorliegenden Beispiel als Sensor zur Erkennung eines Fingerabdrucks samt der dafür notwendigen Auswerteeinrichtung ausgeführt. In einer vereinfachten Ausführung könnte hier aber auch eine Paßwort-Eingabe erfolgen. Nach Eingabe des Paßwortes bzw. Auflegen eines Fingers und Erkennung des Fingerabdrucks eines berechtigten Benutzers erzeugt der Identifizierungs-Computer **9** einen Paßwortzahlencode. Gemeinsam mit diesem werden in dem Identifizierungs-Computer **9** gespeicherte Zugangsdaten zu dem lokalen Computernetzwerk an den Einzelrechner **5** über die Kommunikationsschnittstelle **8** und **7** übermittelt. Die Verbindung **11** zwischen diesen beiden Kommunikationsschnittstellen **7** und **8** ist in besonders einfacher Weise durch eine Blue Tooth-Schnittstelle realisiert. Schnittstellen nach dem Blue Tooth-Industriestandard können auch für andere Anwendungen verwendet werden, so daß dies in vielen Fällen keinen zusätzlichen Aufwand an dem Einzelrechner bedeutet. Zusammen mit dem Paßwortzahlencode und den

Zugangsdaten wird ein Steuerbefehl an den Einzelrechner übermittelt. Eine dafür vorgesehene Software auf dem Einzelrechner **5** startet nun den Verbindungsaufbau zu dem lokalen Computernetzwerk **1** und führt dort die erforderliche Registrierung durch. Dem Benutzer ist es somit möglich, lediglich durch das Auflegen eines Fingers auf den Identifizierungs-Computer einen vollständigen Verbindungsaufbau und die Registrierung beim lokalen Computernetzwerk **1** durchzuführen, wobei die unberechtigte Benutzung durch Dritte verhindert ist.

## Patentansprüche

1. Netzwerkanordnung mit
einem lokalen Computernetzwerk (**1**),
einem Einzelrechner (**5**), der Mittel (**12**) zum Aufbau einer Verbindung (**6**) zum lokalen Computernetzwerk aufweist, und
einem Identifizierungs-Computer (**9**), der über eine Kommunikationsschnittstelle (**7, 8**) mit dem Einzelrechner (**5**) Daten austauschen kann,
wobei in dem Identifizierungs-Computer (**9**) Zugangsdaten zu dem lokalen Netzwerk (**1**) gespeichert oder erzeugbar sind und wobei auf Übermittlung eines Steuerbefehls von dem Identifizierungs-Computer (**9**) an den Einzelrechner (**5**) ein Verbindungsaufbau zwischen dem Einzelrechner (**5**) und dem lokalen Computernetzwerk (**1**) und eine Registrierung im lokalen Computernetzwerk (**1**) mit den Zugangsdaten durchgeführt werden.

2. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß der Identifizierungs-Computer (**9**) eine Benutzerauthentisierungseinheit (**10**) mit einem biometrischen Sensor, vorzugsweise einem Sensor zur Erkennung eines Fingerabdrucks, aufweist.

3. Anordnung nach Anspruch 1, dadurch gekennzeichnet, daß die Kommunikationsschnittstelle (**7, 8**) eine Blue Tooth-Schnittstelle ist.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 100 40 855 A1
Int. Cl.[7]: G 06 F 12/14
Offenlegungstag: 14. März 2002